APPENDIX

INDEX TO APPENDIX

October 3, 2017, 12:30 PM   **Restore this version**

Version history

🖨 90% ▾   Total: 2 edits   ⌃ ⌄   Only show named versions   ⬤

4.0 Performance Measurements

Metric	Description	Current	Target
Network Availability	Percentage of total time* that the infrastructure is functional and reachable via the network	99.50%[1]	99.90%
Resource Availability	Percentage of total time* that resources (computing, storage, database, etc.) are functional and accessible	98.50%[2]	99.90%
Virtual Machine Provisioning Time	Time Until Live for a new virtual machine (once the request has been submitted)		2 min
Storage Provisioning Time	Time Until Live for a new storage container or virtual disk (once the request has been submitted)		2 min
Monitoring Alert Delay	Time between when a problem occurs, to when an automated monitoring system detects the issue and sends a notification to the end-user	N/A	60 sec
Data Analysis Across	Infrastructure enables automated data		

---

[1] "Terms and Conditions - Defense Information Systems Agency." 1 Jun. 2017, http://www.disa.mil/~/media/files/disa/services/computing/termsandconditions.pdf. Accessed 27 Sep. 2017.
[2] "Telecommunications Service Level Agreement (SLA) - Defense ...." 9 Dec. 2016, http://www.disa.mil/~/media/Files/DISA/Services/Network-Services/SLA/TelecommunicationsSLA.pdf. Accessed 27 Sep. 2017.

▸ October 3, 2017, 2:44 PM
  ⬤ Sharon Woods

▸ October 3, 2017, 1:36 PM
  ⬤ Jordan Kasper

▸ **October 3, 2017, 12:30 PM**   ⋮
  ⬤ Sharon Woods
  ⬤ Jordan Kasper

▸ October 3, 2017, 10:18 AM
  ⬤ Sharon Woods

October 2, 2017, 9:58 AM
  ⬤ Sharon Woods

▸ October 2, 2017, 9:04 AM
  ⬤ Sharon Woods

SEPTEMBER 2017

▸ September 29, 2017, 4:22 PM
  ⬤ Sharon Woods

▸ September 29, 2017, 9:49 AM
  ⬤ Sharon Woods

September 29, 2017, 9:16 AM

☑ Show changes

App. 1

October 3, 2017, 12:30 PM   **Restore this version**

Version history

🖨   75% ▼   Total: 2 edits   ∧ ∨

Only show named versions

▸ October 3, 2017, 2:44 PM
   ● Sharon Woods

▸ October 3, 2017, 1:36 PM
   ● Jordan Kasper

▸ **October 3, 2017, 12:30 PM**   ⋮
   ● Sharon Woods
   ● Jordan Kasper

▸ October 3, 2017, 10:18 AM
   ● Sharon Woods

October 2, 2017, 9:58 AM
   ● Sharon Woods

▸ October 2, 2017, 9:04 AM
   ● Sharon Woods

SEPTEMBER 2017

▸ September 29, 2017, 4:22 PM
   ● Sharon Woods

▸ September 29, 2017, 9:49 AM
   ● Sharon Woods

September 29, 2017, 9:16 AM

☑ Show changes

Disparate Data Sets	analysis across disparate data sets regardless of organizational boundaries		
Data exchange across classification levels			
Elapsed Time to Identify Failure (ETIF) and Elapsed Time to Identify Threat (ETIT)	on-cloud automated AI agents that are able to detect anomalies in behavior and network activity at machine speed		
Incident Response:			
Time to Detect (T_0)	The window of time between a compromise and the detection of a threat	seconds to minutes, <60	
Time to Confirm (T_{-1})	Time it takes to make a decision- ensuring the alert was not a false positive, escalation or assignment of task	seconds to minutes,< 60	
Time to Contain (T_{-2})	Time to Compartmentalize and conduct forensics of intrusion set	seconds to hours,<12	
Time to Remove (T_{-3})	Time required to Expunge / Purge intrusion set	Seconds to hours, < 12	
Operational Availability (T_{-4})	Delta between (T_0) and (T_{-4})		
User Account creation			
Availability of automated managed services on a platform across classification levels			

* Less scheduled downtime

App. 2

IN THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST

ORACLE AMERICA, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	
THE UNITED STATES,	)	
	)	No. 18-1880C
Defendant,	)	(Senior Judge Bruggink)
	)	
and	)	
	)	
AMAZON WEB SERVICES, INC.,	)	
	)	
Defendant-Intervenor.	)	

DECLARATION OF LIEUTENANT GENERAL BRADFORD J. SHWEDO

I, Lieutenant General Bradford J. Shwedo, United States Air Force, declare as follows:

1.   I am the Director for Command, Control, Communications, and Computers/Cyber (C4), Chief Information Officer, Joint Staff. I develop C4 capabilities; conduct analysis and assessments; provide Joint and Combined Force C4 guidance; and evaluate C4 requirements, plans, programs and strategies for the Chairman of the Joint Chiefs of Staff.

2.   In my capacity with the Joint Staff, I am familiar with the Joint Enterprise Defense Infrastructure (JEDI) Cloud acquisition and can explain the urgency and importance of this requirement.

3.   The Department of Defense has entered the modern age of warfighting where the battlefield exists as much in the digital world as it does in the physical. New commercial technology will change society, and ultimately, the character of war by making data weaponized (e.g., controlling the flow of information in and out of a battlespace to gain a strategic edge or

1

App. 3

multi-domain command and control where air, sea, ground and space networks are merged to give commanders a comprehensive, up-to-the-minute picture of the battlefield), rather than traditional weapons platforms, the decisive factor in defense of the nation. As data increases in size and complexity, our current compartmentalized management of data is untenable to assist our warfighters at the speed of relevance. We must relentlessly pursue innovative digital solutions for national security to maintain military dominance over our adversaries, who are also weaponizing the use of their data. For example, in February 2017, Russian Defense Minister openly acknowledged the formation of an Information Army within the Russian military. JEDI Cloud is critical to safeguarding our technological advantage against those that seek to harm our nation.

JEDI Cloud is the Department's leading effort to create a global cloud capability at all classification levels across the Enterprise to the Warfighter. As described in DoD's 2019 Cloud Strategy, JEDI Cloud is a general purpose, enterprise-wide cloud that is critical to the Department's future. Successful implementation of JEDI Cloud will enhance lethality and strategic readiness. JEDI Cloud will enable the warfighter to quickly convert data to actionable information, which is recognized as critical by all of the combatant commands. Three examples of the impact that I expect JEDI Cloud will have are provided below.

4.   Example 1: Currently, due to the lack of a globally available general purpose cloud, a significant amount of information that is collected from surveillance equipment, such as surveillance aircraft, is never analyzed. In fact, much of our information is unused because the Department does not have enough readily available server capacity to electronically store the data, wasting valuable opportunities to gain military advantage. Because commercial cloud is elastic, meaning that storage and computing power can rapidly be made available within moments, JEDI Cloud should provide a global platform that solves the problem of insufficient storage to host all

2

App. 4

of the information gathered from surveillance equipment. Moreover, having an enterprise-wide cloud environment enables the data to be aggregated. Once aggregated, advanced analysis capabilities like Artificial Intelligence (AI) and Machine Learning (ML) can be used to ensure the warfighters are receiving analyzed data in a reduced amount of time. Any delays in the adoption of JEDI Cloud delays our warfighters from receiving information that could make the difference in successfully completing missions and getting home to their families.

5.　　　Example 2: Much of the technology that the military uses to conduct missions relies upon communication links to function. Consequently, our contingency war plans must include the ability to enable our military equipment to function even without traditional forms of communication links, like fiber connections or satellite, because our adversaries could seek to disrupt communications by cutting fiber communications connections. This is especially relevant for the Korean peninsula where communications are vulnerable because the communications cables that connect South Korea to the United States can be severed. If communications links are severed, military equipment that is dependent on those connections will be degraded or prevented from working entirely. To overcome this problem, JEDI Cloud will include cloud capabilities that are able to operate out of standalone, portable hardware even when there is no communication link, and that will re-sync with the rest of the global JEDI Cloud quickly when any communication link is re-established. This means that if the communication link with the larger cloud is severed, local military equipment that is connected to the standalone JEDI Cloud hardware could still operate and be used to execute missions. It also means that information globally collected and analyzed, as described in example 1, after the link is disrupted would be quickly available to those in Korea when a link is re-established. Communications vulnerability in Korea is a significant risk.
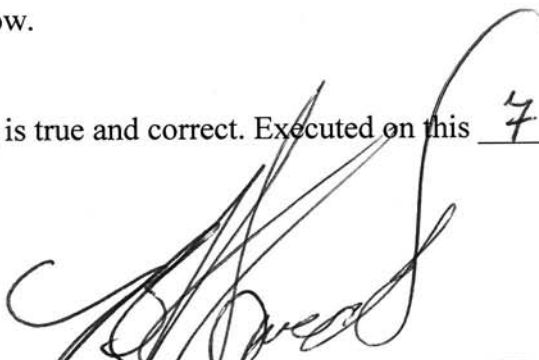
3

App. 5

Mitigating this risk would provide a huge military advantage in a currently contentious region, and any delays will harm the military's ability to achieve national defense in that region.

6.   Example 3: Increasing our force readiness, meaning the number of ready and able warfighters to deploy with the right equipment, is critical to defending this nation. Two key factors that affect force readiness are: a) training, because warfighters require extensive training to be effective, and b) equipment maintenance, because improperly maintained equipment could fail at a time of need. I expect that JEDI Cloud will improve force readiness as it relates to both of these factors. For training, two limiting factors are physically getting everyone to the training location and effectively using the military's massive amounts of data to create realistic training scenarios. New capabilities are being developed today to provide virtual training, but these capabilities require access to massive amounts of elastic storage and computing power, which DoD does not consistently have around the country, let alone on a global basis. Additionally, using data to derive realistic training scenarios requires massive amounts of elastic storage and computing power to analyze that data and derive the training scenarios. JEDI Cloud will provide the necessary amount of elastic storage and computing power, solving both of these challenges simultaneously. In addition, JEDI Cloud should enable these scenarios to include data from the entire enterprise in a more efficient manner. For equipment maintenance, there are incredibly powerful AI algorithms that can be used to predict pre-emptive actions; for example, when an aircraft will require maintenance before anything goes wrong. Running those algorithms and storing the data that is analyzed by the algorithms requires massive amounts of elastic computing power and storage. Again, DoD does not consistently have access to the commercial cloud capabilities that provide the necessary amount of elastic computing power and storage. Both the training and maintenance

4

App. 6

teams are eagerly awaiting the availability of JEDI Cloud in order to move their programs forward. A delay in JEDI Cloud will directly impact these force readiness efforts.

7.   We cannot expect success fighting tomorrow's conflicts with yesterday's technology. Providing the Department rapid access to enterprise cloud, providing elastic computing power and storage, is vital to national security. The men and women of the Joint Force must have access to the right technology at the right time to fight and win wars. Delaying implementation of the JEDI Cloud will negatively impact our efforts to plan, fight, and win in communications compromised environments, and will negatively impact our efforts to improve force readiness and hamper our critical efforts in AI. This position has been forwarded and is supported by all of the U.S. Combatant Commands. Our adversaries are employing these technologies; our warfighters need this capability now.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this __7__ day of June, 2019.

BRADFORD J. SHWEDO
Lieutenant General, USAF
Director for Command, Control,
Communications, and Computers/Cyber,
Chief Information Officer

5

App. 7